ELSEVIER
Theoretical Computer Science 157 (1996) 79–90
Theoretical Computer Science

NC solving of a system of linear ordinary differential equations in several unknowns

D. Grigoriev*,[1]

Departments of Computer Science and Mathematics, Pennsylvania State University, University Park, PA 16802, USA

Abstract

An NC algorithm is described for reducing a system of linear ordinary differential equations in several unknowns to the standard basis form

0. Introduction

We consider a problem of solvability of a system of linear ordinary differential equations in several unknowns

$$\sum_j L_{ij}u_j = b_i \ ,$$

where $b_i \in \mathbb{Q}(X)$ and $L_{ij} = \sum_k f_k(d^k/dX^k)$ are linear ordinary differential operators with the rational coefficients $f_k \in \mathbb{Q}(X)$. We consider a solvability of the system in the unknowns u_j in the differential closure of $\mathbb{C}(X)$ (in fact, as we deal with the linear operators it is equivalent to the solvability in Picard–Vessiot closure of $\mathbb{C}(X)$) (see [10]), in which any (resp. linear) ordinary differential equation has a solution. In other words, solvability in Picard–Vessiot closure means that the system cannot be brought to a contradiction by equivalent transformations over the ring $\mathscr{R} = \mathbb{C}(X)[d/dX]$ of the linear differential operators, or more precisely, that the ideal in the ring of differential polynomials in $\{u_j\}$, generated by the differential polynomials $\{\sum_j L_{ij}u_j - b_i\}$, differs from the unit one.

Remark that this problem is a particular case of the problem of solvability (over differential closure) of a system of non-linear ordinary differential equations in several unknowns (more general, a quantifier elimination problem for these systems), for which an algorithm with elementary complexity (more precisely, double-exponential) was designed in [5]. In the present paper we deal with a linear fragment of this general problem and describe for it an algorithm with a considerably better (than for the general

* e-mail: dima@math.psu.edu.
[1] Supported in part by NSF grant CCR-9424358.

SSDI 0304-3975(95)00176-X

problem) complexity, namely from the complexity class NC, i.e. with polynomial time and polylog depth (parallel time), moreover the algorithm produces a "triangular" basis for the space of solutions of the system.

A close problem to the one under consideration is solving linear system over the ring $\mathscr{R}$ of differential operators for which an algorithm was designed in [8] (even for the case of the differential operators with the coefficients in many variables from $\mathbb{Q}(X_1,\ldots,X_n)$). The problem considered in the present paper is more subtle from the point of view of the allowed transformations of a system since for the sake of equivalence we may not multiply the equations of the system by the differential operators, as we could do in the case of the linear systems over $\mathscr{R}$ (see [8]).

Therefore, we need to carry out elementary transformations with the matrix over $\mathscr{R}$ of the system (see Section 1), in order to reduce the matrix to a standard basis form which is a particular case of a differential standard basis [3, 4, 13] for partial differential operators. Since the ring $\mathscr{R}$ is non-commutative (some of its properties one can find in e.g. [2]), the difficulties arise in estimating the standard basis form of the matrix over $\mathscr{R}$ unlike the case of the matrices over the (euclidean) rings of integers or univariate polynomials, because for the latter one exploits the notion of the determinant. But still we are able (see Lemma 4) to bound the size of a quasi-inverse of a matrix over $\mathscr{R}$ (for an invertible matrix a similar bound follows from the bound in [13] obtained for a more general situation of non-linear operators) and define the rank of a matrix over $\mathscr{R}$ (see [9], also Lemma 5 below). To replace the notion of the determinant we consider (see Section 2) the order [14] of a system of linear differential operators, i.e. of a matrix over $\mathscr{R}$, being the dimension over $\mathbb{C}(X)$ of the factor-module of the free $\mathscr{R}$-module over the submodule generated by the rows of the matrix. We prove that the order is additive with respect to the product of the square matrices (Lemmas 6 and 7). Relying on Lemma 7, on the analogue of Bezout's theorem for differential equations [11, 14] (see also Lemma 9) and on a bound on a quasi-inverse matrix (see Lemma 4 in Section 1), we estimate in Section 3 the size of the standard basis form of the matrix (see Lemma 10) using the construction of a minimal element in a module with respect to a non-archemedian form (the order). In the last Section 4 we give an algorithm from NC for constructing the standard basis form of a matrix, applying the bounds achieved in Section 3. This provides a desired algorithm from NC for testing solvability of a system of linear ordinary differential equations and producing a "triangular" basis for the space of solutions of a system (see the theorem in Section 4).

Let us underline that the main purpose of this paper is to describe an algorithm with the low complexity (NC) for an important problem in symbolic computations in systems of linear differential equations. The needed auxiliary bounds from Sections 1 and 2 (unfortunately, nowhere written explicitely) could be obtained without difficulties by the experts in differential algebra and they are included to make the paper self-contained.

We also mention that the problem of solving a single linear ordinary differential equation in one unknown leads to the problem of factoring of the equation; for the latter problem an algorithm was proposed in [6]. A slight generalization of this problem

is solving a first-order system of linear ordinary differential equations, an algorithm for reducing a matrix of this system to the block-triangular form was exhibited in [7]. A connection of the first-order linear systems with the general linear systems considered in the present paper, is discussed in Section 4.

1. Transformations and the rank of matrices over the ring of linear differential operators

Denote by $D = d/dX$, $\mathscr{R} = \mathbb{C}(X)[D]$, and by $\mathscr{F}$ a Picard–Vessiot closure of $\mathbb{C}(X)$ (see [10]), i.e. any linear differential equation $L = \left(\sum_{0\leqslant i\leqslant n} f_i D^i\right) u = 0$ with the coefficients $f_i \in \mathscr{F}$ and the leading coefficient $\ell c(L) = f_n \neq 0$ has n linearly independent over $\mathbb{C}$ solutions in $\mathscr{F}$, and furthermore, a subfield of constants of $\mathscr{F}$ (i.e. the elements $c \in \mathscr{F}$ such that $Dc = 0$) coincides with $\mathbb{C}$.

We consider a problem of solvability in $\mathscr{F}$ of a system of linear ordinary differential equations in several unknowns

$$\sum_{1\leqslant j\leqslant s} L_{ij}u_j = b_i, \quad 1\leqslant i\leqslant k\ , \tag{1}$$

where $L_{ij} \in \mathbb{Q}(X)[D]$, $b_i \in \mathbb{Q}(X)$ and the solutions $u_1,\ldots,u_s$ should be in $\mathscr{F}^s$. For an operator $L = \sum_{0\leqslant i\leqslant n} f_i D^i \in \mathscr{R}$ with $\ell c(L) = f_n \neq 0$ denote $n = \operatorname{ord} L$ and by $\deg L$ denote $\sum_{0\leqslant i\leqslant n} \deg_X f_i$. Consider $k \times s$ matrix $\mathscr{L} = (L_{ij})$, assume that $\operatorname{ord}\mathscr{L}\leqslant r$, $\deg\mathscr{L}\leqslant d$, $\deg(b_i)\leqslant d$, i.e. $\operatorname{ord} L_{ij}\leqslant r$, $\deg L_{ij}\leqslant d$ for all i,j. Assume also that the bit-size of each (rational) coefficient of L_{ij}, b_i does not exceed M.

Consider now $k \times s$ matrix $A = (A_{ij})$ with the entries $A_{ij} \in \mathscr{R}$, assume that $\operatorname{ord}(A_{ij})\leqslant r$. As the ring $\mathscr{R}$ is left-euclidean, making elementary transformations over $\mathscr{R}$ with the rows, one can reduce A to the following standard basis form, see [9] (it is a particular case of a characteristic set [14] which is considered in [14] in nonlinear case, or of a differential standard basis [3, 4, 13])

$$Q = \begin{pmatrix} 0 & \ldots & 0Q_{1p_1} & & & & & \\ 0 & \ldots & \ldots & 0Q_{2p_2} & & & & \\ 0 & \ldots & \ldots & \ldots & 0Q_{3p_3} & * & & \\ \vdots & & & & \ddots & & & \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & 0Q_{\ell,p_\ell} & \ldots \\ & & & \bigcirc & & \bigcirc & & \end{pmatrix}, \tag{2}$$

where $p_1 < p_2 < \cdots < p_\ell$, all the rows starting with $(\ell+1)$-th vanish . Let us admit also as an elementary transformation the multiplication (from the left) of a row by a non-zero element from $\mathbb{C}(X)$. In other words, there is $k \times k$ matrix $B = (B_{ij})$ over $\mathscr{R}$ being a product of elementary matrices such that $BA = Q$. The rows of Q provide a triangular basis of a left $\mathscr{R}$-module $\mathscr{R}^k A \subset \mathscr{R}^s$ generated by the rows of the matrix A.

The next lemma and the corollary one can deduce from the results in [9].

Lemma 1. *A square $k \times k$ matrix A over $\mathscr{R}$ is invertible from the left if and only if A equals to a product of elementary matrices.*

Corollary. *A square matrix is invertible from the left if and only if it is invertible from the right. The left inverse is unique and coincides with the right inverse. Thus, one could talk simply about invertible matrices.*

We say that $k \times s$ matrix A is quasi-invertible from the left if there exists $s \times k$ matrix G over $\mathscr{R}$ such that

$$GA = \begin{pmatrix} C_1 & & \bigcirc \\ & \ddots & \\ \bigcirc & & C_s \end{pmatrix}$$

is a diagonal matrix with non-zero diagonal elements $C_1, \ldots, C_s$ (in a similar way one could define quasi-invertibility from the right).

Lemma 2. *A is quasi-invertible from the left iff the dimension $\dim_{\mathbb{C}(X)}(\mathscr{R}^s/\mathscr{R}^k A) < \infty$ of the factor-module is finite.*

Proof. If

$$GA = \begin{pmatrix} C_1 & & \bigcirc \\ & \ddots & \\ \bigcirc & & C_s \end{pmatrix}$$

and $\operatorname{ord} C_1 = r_1, \ldots, \operatorname{ord} C_s = r_s$ then the vectors

$$\Pi(e_i^{(j)}) = \Pi(\underbrace{0, \ldots, 0, D^j}_{i}, 0, \cdots, 0) \in \mathscr{R}^s/\mathscr{R}^k A$$

for $1 \leqslant i \leqslant s$, $0 \leqslant j < r_i$ constitute a generating set over $\mathbb{C}(X)$ of $\mathscr{R}$-module $\mathscr{R}^s/\mathscr{R}^k A$, where $\Pi : \mathscr{R}^s \to \mathscr{R}^s/\mathscr{R}^k A$, is the natural projection, hence $\dim_{\mathbb{C}(X)}(\mathscr{R}^s/\mathscr{R}^k A) \leqslant r_1 + \cdots + r_s$ (for a better inequality see Lemmas 9 and 10).

Let $\dim_{\mathbb{C}(X)}(\mathscr{R}^s/\mathscr{R}^k A) < \infty$. Then one can reduce A by elementary transformations of the rows to standard basis form (2) and if $\ell < s$ then the infinite family of vectors $\Pi(e_p^{(0)})$, $\Pi(e_p^{(1)}), \ldots$, where $1 \leqslant p \leqslant s$ is distinct from $p_1, \ldots, p_\ell$, are independent over $\mathbb{C}(X)$ and we get a contradiction. Therefore, $\ell = s$. One can show that there exists $s \times k$ matrix G over $\mathscr{R}$ such that

$$GQ = \begin{pmatrix} C_1 & & \bigcirc \\ & \ddots & \\ \bigcirc & & C_s \end{pmatrix}$$

with non-zero $C_1, \ldots, C_s$. Indeed, multiply the first row of Q by a suitable element $0 \neq \alpha_1 \in \mathscr{R}$ such that $\alpha_1 Q_{12} = \beta_1 Q_{22}$ for a certain $\beta_1 \in \mathscr{R}$ (this is possible since $\mathscr{R}$ is an Ore domain [2]), then subtract from the first row the second one multiplied by β_1, thereby we will achieve the vanishing of the entry with the coordinates (1, 2).

Continuing in a similar way, we will make all the entries in the first row (except the diagonal entry) to be zeroes. Then we proceed to the second row and so on. As a result we will get a diagonal matrix which shows that A is quasi-invertible from the left. □

Observe that when $\dim_{\mathbb{C}(X)}(\mathscr{R}^s/\mathscr{R}^k A) < \infty$, the latter dimension coincides with the order of the system $Au = 0$ [14]. In [14] the order was introduced for a prime ideal in the ring of differential polynomials, we use it for a linear ideal generated by the rows of A.

The next lemma was actually proved in [8].

Lemma 3. *A is quasi-invertible from the left iff there does not exist a vector $0 \neq v \in \mathscr{R}^s$ such that $Av = 0$. For $(s-1) \times s$ matrix A one can select $0 \neq v \in \mathscr{R}^s$ such that $Av = 0$ and $ord(v) \leqslant (s-1)r + 1$.*

Proof. If A is quasi-invertible from the left and

$$GA = \begin{pmatrix} C_1 & & \bigcirc \\ & \ddots & \\ \bigcirc & & C_s \end{pmatrix}$$

then $Av \neq 0$ for any $0 \neq v \in \mathscr{R}^s$ as $\mathscr{R}$ has no divisors of zero ([2]).

Conversely, let $Av \neq 0$ for any $0 \neq v \in \mathscr{R}^s$. Let us show that in the standard basis form (2) $\ell = s$. Suppose $\ell < s$. Consider the $\mathbb{C}(X)$-space $\mathscr{R}^{s;N}$ of the vectors $(\alpha_1, \ldots, \alpha_s) \in \mathscr{R}^s$ for which $\operatorname{ord}(\alpha_1), \ldots, \operatorname{ord}(\alpha_s) < N$. Let $\operatorname{ord}(Q_{ij}) \leqslant R$ for all i, j. Then the composition of the mapping $Q : v \to Qv$ with the restriction onto first ℓ coordinates (notice that others are zeroes, see (2)) maps $\bar{Q} : \mathscr{R}^{s;N} \to \mathscr{R}^{\ell;N+R}$. As $\dim_{\mathbb{C}(X)} \mathscr{R}^{s;N} = sN$, for $N = [\ell R/(s-\ell)] + 1$ we get that $\dim_{\mathbb{C}(X)} \mathscr{R}^{s;N} > \dim_{\mathbb{C}(X)} \mathscr{R}^{\ell;N+R}$ and therefore, there exists a vector $0 \neq v \in \mathscr{R}^{s;N}$ such that $Qv = 0$, hence $BAv = 0$ and thus $Av = 0$ since B is a product of elementary matrices (cf. Lemma 1). The obtained contradiction with the supposition justifies the equality $\ell = s$. Then one can show that A is quasi-invertible from the left. This proves the first statement of the lemma. For the second statement follow the latter proof considering instead of $\bar{Q}$ the mapping $\bar{A} : \mathscr{R}^{s;M} \to \mathscr{R}^{s-1;M+\operatorname{ord}(A)}$ for $M = (s-1)\operatorname{ord} A + 1$. □

The next lemma was proved in [8].

Lemma 4. *A square $s \times s$ matrix A is quasi-invertible from the left iff A is quasi-invertible from the right. In this case there exists G for which*

$$GA = \begin{pmatrix} C_1 & & \bigcirc \\ & \ddots & \\ \bigcirc & & C_s \end{pmatrix}$$

with $ord(G) \leqslant (s-1)r + 1$.

Proof. Let A be quasi-invertible from the left. Then for an appropriate matrix B, being a product of elementary matrices, we have

$$BA = \begin{pmatrix} Q_{11} & Q_{12} & & \\ & \ddots & \ddots & \\ \bigcirc & & & Q_{ss} \end{pmatrix}$$

where $Q_{11} \cdots Q_{ss} \neq 0$ (see (2) and the proof of Lemma 2). Let us show that for any vector $0 \neq w \in \mathscr{R}^s$ holds $wA \neq 0$, this would imply that A is quasi-invertible from the right because of Lemma 3. Assume that $0 = wA$. Then $0 = wA = (wB^{-1}Q)$ and we get a contradiction, which justifies that A is quasi-invertible from the right.

In order to prove the necessary bound on G, consider for each $1 \leqslant j \leqslant s$ a matrix $A^{(j)}$ obtained from A by deleting its jth column. Lemma 3 shows that there exists a vector $0 \neq g^{(j)} \in \mathscr{R}^s$ such that $g^{(j)}A^{(j)} = 0$ and $\operatorname{ord} g^{(j)} \leqslant (s-1)r + 1$. As a matrix G take a matrix with jth row equal to $g^{(j)}$. □

Notice that when A is invertible, Lemma 4 follows from the Theorem 6 of [13], where a similar bound was proved for a much more general situation of an invertible non-linear differential map.

Thus, for a square matrix A we can say that it is quasi-invertible without specifying from the left or from the right. Notice (see also [8]) that a square matrix A is quasi-invertible iff its Dieudonné determinant ([1]) does not vanish.

Define the rank $rk(A)$ as a maximal ℓ such that there exists $\ell \times \ell$ quasi-invertible submatrix of A (cf. [9]), the following lemma can be deduced from the results in [9].

Lemma 5. *$rk(A)$ coincides with*

(a) *ℓ in the standard basis form* (2);

(b) *the maximal number of the columns of A being $\mathscr{R}$-linearly independent;*

(c) *the maximal number of the rows of A being $\mathscr{R}$-linearly independent.*

2. Some properties of the order of a system of linear differential operators

For brevity we adopt the notation $\dim(\mathscr{R}^s/\mathscr{R}^k A) = \dim_{\mathbb{C}(X)}(\mathscr{R}^s/\mathscr{R}^k A)$.

Lemma 6. *For any $m \times k$ matrix B and $k \times s$ matrix A over $\mathscr{R}$*

$$\dim(\mathscr{R}^s/\mathscr{R}^m BA) \leqslant \dim(\mathscr{R}^k/\mathscr{R}^m B) + \dim(\mathscr{R}^s/\mathscr{R}^k A)\ .$$

If A is quasi-invertible from the right then this inequality turns to be the equality.

Proof. Consider the natural projections

$$\Pi_1 : \mathscr{R}^s \to \mathscr{R}^s/\mathscr{R}^k A, \qquad \Pi_2 : \mathscr{R}^k \to \mathscr{R}^k/\mathscr{R}^m B, \qquad \Pi_3 : \mathscr{R}^s \to \mathscr{R}^s/\mathscr{R}^m BA.$$

Let $u_1, \ldots, u_\gamma \in \mathscr{R}^k$ be such that $\Pi_2(u_1), \ldots, \Pi_2(u_\gamma)$ constitute a basis over $\mathbb{C}(X)$

of $\mathscr{R}^k/\mathscr{R}^m B$, and $v_1,\ldots,v_\delta \in \mathscr{R}^s$ be such that $\Pi_1(v_1),\ldots,\Pi_1(v_\delta)$ constitute a basis over $\mathbb{C}(X)$ of $\mathscr{R}^s/\mathscr{R}^k A$ (note that γ or δ could be infinite). Let us prove that $\Pi_3(v_1),\ldots,\Pi_3(v_\delta),\Pi_3(u_1A),\ldots,\Pi_3(u_\gamma A)$ generate $\mathscr{R}^s/\mathscr{R}^m BA$ over $\mathbb{C}(X)$ and constitute a basis when A is quasi-invertible from the right. Indeed, let for some elements $f_1,\ldots,f_\delta,\ g_1,\ldots,g_\gamma \in \mathbb{C}(X)$ and a vector $(\beta_1,\ldots,\beta_m) \in \mathscr{R}^m$ we have $f_1v_1+\cdots+f_\delta v_\delta+(g_1u_1+\cdots+g_\gamma u_\gamma)A=(\beta_1,\ldots,\beta_m)BA$, then $f_1=\cdots=f_\delta=0$. If A is quasi-invertible from the right then $g_1u_1+\cdots+g_\gamma u_\gamma=(\beta_1,\ldots,\beta_m)B$ by virtue of Lemma 3, hence $g_1=\cdots=g_\gamma=0$.

On the other hand, for any vector $w \in \mathscr{R}^s$ there exist $f_1,\ldots,f_\delta \in \mathbb{C}(X)$ and a vector $v \in \mathscr{R}^k$ for which $w=f_1v_1+\cdots+f_\delta v_\delta+vA$. Then $v=g_1u_1+\cdots+g_\gamma u_\gamma+uB$ for suitable $g_1,\ldots,g_\gamma \in \mathbb{C}(X)$, $u \in \mathscr{R}^m$. Therefore $w=f_1v_1+\cdots+f_\delta v_\delta+g_1u_1A+\cdots+g_\gamma u_\gamma A+uBA$, i.e. $\dim(\mathscr{R}^s/\mathscr{R}^m BA)\leqslant\gamma+\delta=\dim(\mathscr{R}^k/\mathscr{R}^m B)+\dim(\mathscr{R}^s/\mathscr{R}^k A)$. □

In other terms we can reformulate what was proved above, saying that we have the following exact sequence of $\mathbb{C}(X)$-vector spaces

$$\mathscr{R}^k/\mathscr{R}^m B \xrightarrow{\alpha} \mathscr{R}^s/\mathscr{R}^m BA \xrightarrow{\pi} \mathscr{R}^s/\mathscr{R}^k A \to O$$

where $\alpha(v+\mathscr{R}^m B)=vA+\mathscr{R}^m BA$ and $\pi(w+\mathscr{R}^m BA)=w+\mathscr{R}^k A$. In the case of quasi-invertible A the following sequence is exact:

$$O \to \mathscr{R}^k/\mathscr{R}^m B \xrightarrow{\alpha} \mathscr{R}^s/\mathscr{R}^m BA \xrightarrow{\pi} \mathscr{R}^s/\mathscr{R}^k A \to O$$

Lemma 7. *If a matrix A is square then* $\dim(\mathscr{R}^s/\mathscr{R}^m BA)=\dim(\mathscr{R}^s/\mathscr{R}^m B)+\dim(\mathscr{R}^s/\mathscr{R}^s A)$.

Proof. If A is quasi-invertible (see Lemma 4) then we use Lemma 6. If A is not quasi-invertible then $\dim(\mathscr{R}^s/\mathscr{R}^m BA)\geqslant\dim(\mathscr{R}^s/\mathscr{R}^s A)=\infty$. □

We remark here that as in the following example

$$\dim\left(\mathscr{R}^2/\mathscr{R}^2\begin{pmatrix}1&1\\1&D\end{pmatrix}\right)=1,\quad \dim\left(\mathscr{R}/\mathscr{R}^2\begin{pmatrix}1\\1\end{pmatrix}\right)=0$$

and for the product of these matrices

$$\dim\left(\mathscr{R}/\mathscr{R}^2\begin{pmatrix}2\\1+D\end{pmatrix}\right)=0,$$

the inequality in Lemma 6 for rectangular matrices could be strict.

Lemma 8. (a) *For a triangular $k\times s$ (where $k\geqslant s$) matrix*

$$C=\begin{pmatrix}C_1&&*\\&\ddots&\\O&&C_s\end{pmatrix}$$

we have $\dim(\mathscr{R}^s/\mathscr{R}^k C)=\operatorname{ord}C_1+\cdots+\operatorname{ord}C_s$, *provided that* $C_1\cdots C_s\neq 0$.

(b) $\dim(\mathscr{R}^s/\mathscr{R}^k A) < \infty$ *iff* $\ell = s$ *in the standard basis form* (2). *In this case* $\dim(\mathscr{R}^s/\mathscr{R}^k A) = \operatorname{ord} Q_{11} + \cdots + \operatorname{ord} Q_{ss}$.

(c) *When* A *is a square matrix then* $\dim(\mathscr{R}^s/\mathscr{R}^s A) = \dim(\mathscr{R}^s/A\mathscr{R}^s)$, *where in the right side of the equality we regard* $\mathscr{R}^s$ *as a right* $\mathscr{R}$*-module.*

(d) A *square matrix* A *is invertible iff* $\dim(\mathscr{R}^s/\mathscr{R}^s A) = 0$.

Proof. (a) Is obvious.

(b) The first statement one can find in the proof of Lemma 3. The second statement follows from (a) and the equality $\dim(\mathscr{R}^s/\mathscr{R}^k A) = \dim(\mathscr{R}^s/\mathscr{R}^k Q)$.

(c) Because of Lemma 4 both left and right sides of the equality are finite or infinite simultaneously. Assume they are both finite. Then

$$BA = \begin{pmatrix} Q_{11} & * & \\ & \ddots & \\ \bigcirc & & Q_{ss} \end{pmatrix}$$

(see (2)) where B is a product of elementary matrices and $Q_{11} \cdots Q_{ss} \neq 0$ (see (b)). For any $s \times s$ elementary matrix G we have $\dim(\mathscr{R}^s/\mathscr{R}^s G) = \dim(\mathscr{R}^s/G\mathscr{R}^s) = 0$, hence by Lemma 7 the same is true for any invertible matrix (cf. Lemma 1), thus $\dim(\mathscr{R}^s/\mathscr{R}^s B) = \dim(\mathscr{R}^s/B\mathscr{R}^s) = 0$. (a) implies that for the triangular matrix

$$Q = \begin{pmatrix} Q_{11} & * & \\ & \ddots & \\ \bigcirc & & Q_{ss} \end{pmatrix}$$

the equalities $\dim(\mathscr{R}^s/\mathscr{R}^s Q) = \dim(\mathscr{R}^s/Q\mathscr{R}^s) = \operatorname{ord} Q_{11} + \cdots + \operatorname{ord} Q_{ss}$ hold, then Lemma 7 entails (c).

(d) follows from (b) and Lemma 1. □

The following lemma was proved in [14, p. 135], (see also [11]) in a more general form for the order of a prime ideal in the ring of differential polynomials.

Lemma 9. *If* $k \times s$ *matrix* A *is quasi-invertible from the left then* $\dim(\mathscr{R}^s/\mathscr{R}^k A) \leqslant \max_i \{\operatorname{ord} a_{i1}\} + \cdots + \max_i \{\operatorname{ord} a_{is}\}$.

3. Bounds on the standard basis form of a matrix over the ring of differential operators

In this section we will estimate $\operatorname{ord}(Q)$, $\operatorname{ord}(B)$ in the standard basis form (2) relying on the results on the order from the Section 2.

Take any $s \times s$ permutation matrix P, mapping $P(p_1) = 1, \ldots, P(p_\ell) = \ell$, then

$$BAP = \begin{pmatrix} Q_{1p_1} & & & \\ & \ddots & & \\ & & Q_{\ell p_\ell} & \cdots \\ \bigcirc & & \bigcirc & \end{pmatrix}.$$

Represent $AP = (A_1 A_2)$ where $k \times \ell$ submatrix A_1 consists of the first ℓ columns of AP, then by Lemma 5, $rkA = rkA_1 = \ell$. Complete A_1 by $(k - \ell)$ columns of the type $(0, \ldots, 0, 1, 0, \ldots, 0)^{\mathrm{T}}$ to $k \times k$ quasi-invertible matrix $(A_1 A_3)$. Then

$$B(A_1 A_3) = \begin{pmatrix} Q_{1p_1} & & & \\ & \ddots & & \\ & & Q_{\ell p_\ell} & \\ & \bigcirc & & * \end{pmatrix}.$$

Making several elementary transformations with the rows having indices larger than ℓ, reduce the matrix at the right side to the triangular form

$$B_0(A_1 A_3) = \begin{pmatrix} Q_{1p_1} & & & * & \\ & \ddots & & & \\ & & Q_{\ell p_\ell} & & \\ & & & Q^{(0)}_{\ell+1,\ell+1} & \\ & \bigcirc & & & \ddots \\ & & & & Q^{(0)}_{kk} \end{pmatrix}$$

herewith $B = \binom{B_1}{B_2}$ where B_1 is $\ell \times k$ submatrix, $B_0 = \binom{B_1}{B_3}$ and $\dim(\mathscr{R}^k/\mathscr{R}^k B) = \dim(\mathscr{R}^k/\mathscr{R}^k B_0) = 0$ (see Lemma 8(d)).

Moreover, making some elementary transformations with the rows, one can assume w.l.o.g. that $\operatorname{ord}(Q_{ip_i}) < \operatorname{ord}(Q_{jp_i})$, $\operatorname{ord}(Q^{(0)}_{ij}) < \operatorname{ord}(Q^{(0)}_{jj})$ for all $i < j$.

By Lemmas 6, 7 and 9 $\operatorname{ord}(Q_{1p_1}) + \cdots + \operatorname{ord}(Q_{\ell p_\ell}) + \operatorname{ord}(Q^{(0)}_{\ell+1,\ell+1}) + \cdots + \operatorname{ord}(Q^{(0)}_{kk}) = \dim(\mathscr{R}^k/\mathscr{R}^k A_1 A_3) \leqslant \max_i \{\operatorname{ord} A_{ip_1}\} + \cdots + \max_i \{\operatorname{ord} A_{ip_\ell}\} \leqslant \ell r$, hence $\operatorname{ord}(Q_{i,p_i})$, $\operatorname{ord}(Q^{(0)}_{ij}) \leqslant \ell r$. By Lemma 4 there exists $k \times k$ matrix G over $\mathscr{R}$ such that

$$(A_1 A_3)\, G = \begin{pmatrix} C_1 & & \bigcirc \\ & \ddots & \\ \bigcirc & & C_k \end{pmatrix},$$

where $C_1 \cdots C_k \neq 0$ and $\operatorname{ord}(G) \leqslant (k-1)r + 1$, hence $\operatorname{ord}(C_i) \leqslant kr + 1$. As

$$B_0 \begin{pmatrix} C_1 & & \bigcirc \\ & \ddots & \\ \bigcirc & & C_k \end{pmatrix} = \begin{pmatrix} Q_{1p_1} & & & * \\ & \ddots & & \\ & & \ddots & \\ \bigcirc & & & Q^{(0)}_{kk} \end{pmatrix} G,$$

we conclude that $\operatorname{ord}(B_0) \leqslant (\ell + k - 1)r + 1$.

Observe that B_0A has the standard basis form similar to (2) (with the same "diagonal" entries $Q_{1p_1}, \ldots, Q_{\ell,p_\ell}$ and perhaps different other entries as we achieved the conditions $\operatorname{ord} Q_{ip_i} < \operatorname{ord} Q_{jp_j}$, $\operatorname{ord}(Q_{ij}^{(0)}) < \operatorname{ord}(Q_{jj}^{(0)})$, $i < j$)

$$B_0A = \begin{pmatrix} 0 & \ldots & 0\,Q_{1p_1} & & * & \\ 0 & \ldots & \ldots & 0\,Q_{2p_2} & & \\ \vdots & & & \ddots & & \\ 0 & \ldots & \ldots & \ldots & \ldots & 0\,Q_{\ell p_\ell} \\ & & & \bigcirc & & \bigcirc \end{pmatrix}$$

since $rkA = \ell$. Therefore $\operatorname{ord}(Q) \leqslant (\ell + k)r + 1$. Let us summarize what we proved in the present section in the following lemma:

Lemma 10. *There exists an invertible matrix B such that $BA = Q$ has the standard basis form* (2) *and moreover* $\operatorname{ord}(B) \leqslant (s + k - 1)r + 1$, $\operatorname{ord}(Q) \leqslant (s + k)r + 1$.

4. NC algorithm for finding standard basis form of a matrix over the ring of differential operators

Let us design an algorithm which finds the standard basis form of a matrix in NC, i.e. polynomial time and with polylogarithmic depth (parallel complexity).

Join to the matrix A the unit matrix and denote the resulting $k \times (s + k)$ matrix by $\bar{A} = (AE)$. Obviously $rk\bar{A} = k$ (see Lemma 5). Therefore, the standard basis form of $\bar{A}$ equals to

$$B_1\bar{A} = \begin{pmatrix} 0 & \ldots & 0\,Q_{1p_1} & & & & & \\ \vdots & & & \ddots & & & & \\ 0 & \ldots & \ldots & \ldots & 0\,Q_{\ell p_\ell} & * & & \\ \vdots & & & & & \ddots & & \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & 0\,Q_{kp_k} & \ldots \end{pmatrix} = \bar{Q} \quad \text{(see (2))}$$

where $\dim(\mathscr{R}^k/\mathscr{R}^k B_1) = 0$ (see Lemma 8).

For each $1 \leqslant m \leqslant s + k$ and $0 \leqslant j \leqslant (s + 2k)r + 1$ the algorithm tests, whether there exists a vector $w = (w_1, \ldots, w_k)$ with $\operatorname{ord}(w) \leqslant (s + 2k - 1)r + 1$ (cf. Lemma 10) such that the vector

$$w\bar{A} = (\underbrace{0, \ldots, 0}_{m}, v, \ldots)$$

where $\operatorname{ord} v = j$ and the leading coefficient $\ell c(v) = 1$. The latter condition can be written as a linear system $\mathcal{T}_{m,j}$ over $\mathbb{Q}(X)$ with $k((s + 2k - 1)r + 2)$ unknowns being the coefficients of $w_1, \ldots, w_k$ in the powers of $1, D, \ldots, D^{(s+2k-1)r+1}$ and with at most

$(s+k)((s+2k)r+1)$ equations. As the entries of this linear system are the rational functions from $\mathbb{Q}(X)$ with the degrees in X not exceeding d and with the size of rational coefficients at most M, the algorithm can solve $\mathcal{T}_{m,j}$ in time $(Mdskr)^{0(1)}$ with the depth (parallel complexity) $\log^{0(1)}(Mdskr)$ using [12].

As the rows of the matrix $\bar{Q}$ constitute a (triangular) basis of the left $\mathscr{R}$-module $\mathscr{R}^k\bar{A}$, the system $\mathcal{T}_{m,j}$ could be solvable only for $m = p_1,\ldots,p_k$. For each of these $m = p_i$ take the minimal such j_i for which $\mathcal{T}_{p_i,j_i}$ is solvable. Lemma 10 implies that $\mathcal{T}_{p_i,j}$ is solvable for $j = \operatorname{ord} Q_{i,p_i}$, hence $j_i \leqslant \operatorname{ord} Q_{i,p_i}$. Take a solution $W^{(i)} = (w_1^{(i)},\ldots,w_k^{(i)})$ for $\mathcal{T}_{p_i,j_i}$, and denote by W $k\times k$ matrix with ith row to be $W^{(i)}$. Then

$$W\bar{A} = \begin{pmatrix} 0 \ldots 0\,\tilde{Q}_{1p_1} & & \\ \vdots & & * \\ 0 \ldots \quad \ldots & 0\,\tilde{Q}_{kp_k} & \ldots \end{pmatrix} = \tilde{Q},$$

where $\operatorname{ord}\tilde{Q}_{i,p_i} = j_i$.

Let us prove that $\dim(\mathscr{R}^k/\mathscr{R}^kW) = 0$. Denote by $\bar{A}_0,\bar{Q}_0,\tilde{Q}_0$ the $k\times k$ matrices obtained from $\bar{A},\bar{Q},\tilde{Q}$ respectively, by taking the submatrices formed by the columns $p_1,\ldots,p_k$. Then $B_1\bar{A}_0 = \bar{Q}_0$, $W\bar{A}_0 = \tilde{Q}_0$.

Lemmas 7 and 8(a) entail $0 = \dim(\mathscr{R}^k/\mathscr{R}^kB_1) = \operatorname{ord} Q_{1,p_1} + \cdots + \operatorname{ord} Q_{k,p_k} - \dim(\mathscr{R}^{s+k}/\mathscr{R}^k\bar{A}) \geqslant \operatorname{ord}\tilde{Q}_{1,p_1} + \cdots + \operatorname{ord}\tilde{Q}_{k,p_k} - \dim(\mathscr{R}^{s+k}/\mathscr{R}^k\bar{A}) = \dim(\mathscr{R}^k/\mathscr{R}^kW) \geqslant 0$, therefore $\dim(\mathscr{R}^k/\mathscr{R}^kW) = 0$ and moreover $\operatorname{ord}\tilde{Q}_{i,p_i} = \operatorname{ord} Q_{i,p_i}$, $1\leqslant i\leqslant k$. As WA has a desired standard basis form (see (2)), we get the following lemma:

Lemma 11. *There is an* NC*-algorithm, so running in time* $(Mdskr)^{0(1)}$ *with a depth (parallel complexity)* $\log^{0(1)}(Mdskr)$, *which produces an invertible over* $\mathscr{R}$ $k\times k$ *matrix* W *such that*

$$WA = \begin{pmatrix} 0 \quad \ldots \quad 0\,\tilde{Q}_{1p_1} & & & \\ \vdots & & & * \\ 0 \quad \ldots \quad \ldots & & 0\,\tilde{Q}_{\ell p_\ell} & \\ & \bigcirc & & \bigcirc \end{pmatrix}$$

has the standard basis form.

Now we get a criterion for solvability of a system (1). Namely, apply Lemma 11 to $k\times(s+1)$ matrix $A = (L_{ij}\,b_i)_{1\leqslant i\leqslant k,\,1\leqslant j\leqslant s}$, so the last column is

$$\begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}.$$

Then the system (1) has a solution in the field $\mathcal{F}$ iff and only if $p_\ell \leqslant s$ (in other words $p_\ell \neq s+1$) and the standard basis form provides a "triangular" basis of the space

of solutions of (1). Let us summarize what we obtained above in the following main result of the paper:

Theorem. *One can test solvability of a system* (1) *of linear differential equations in several unknowns in the Picard–Vessiot closure* $\mathcal{F}$ *and find a "triangular" basis of the space of solutions of* (1) *in* NC *complexity class, with the time* $(Md\,skr)^{0(1)}$ *and a depth (parallel time)* $\log^{0(1)}(Md\,skr)$.

Observe that the space of solutions of a homogeneous system (1), so when $b_1 = \cdots = b_k = 0$, has a finite dimension (over $\mathbb{C}(X)$) if and only if $p_1 = 1, \ldots, p_\ell = \ell$ and $\ell = s$ (for $k \times s$ matrix $A = (L_{ij})$, see above). In this case the standard basis form WA of the system can be rewritten in the common first-order matrix form $DY = HY$ (cf. [7]), where the vector Y has coordinates $u_1, Du_1, \ldots, D^{j_1-1}u_1, u_2, \ldots, D^{j_2-1}u_2, \ldots, u_s, \ldots, D^{j_s-1}u_s$ and $j_i = \operatorname{ord} \widetilde{Q}_{i,p_i}$, $1 \leqslant i \leqslant s$, one could easily get the matrix H over $\mathbb{Q}(X)$ from the matrix WA.

Acknowledgements

The author would like to thank Mike Singer for his attention to this paper.

References

[1] E. Artin, *Geometric Algebra* (Interscience, New York, 1957).
[2] J.-E. Björk, *Rings of Differential Operators* (North-Holland, Amsterdam, 1979).
[3] G. Carro-Ferro, Groebner Bases and Differential Ideals, in: Lecture Notes Computer Science, Vol. 356 (Springer, New York, 1987) 129–140.
[4] A. Galligo, Some Algorithmic Questions on Ideals of Differential Operators, in: Lecture Notes Computer Science, Vol. 204 (Springer, New York, 1985) 413–421.
[5] D. Grigoriev, Complexity of quantifier elimination in the theory of ordinary differential equations, in: Lecture Notes Computer Science Vol. 378 (Springer, New York, 1989) 11–25.
[6] D. Grigoriev, Complexity of factoring and GCD calculating of ordinary linear differential operators, *J. Symbolic Comput.* **10**(1) (1990) 7–37.
[7] D. Grigoriev, Complexity of irreducibility testing for a system of linear ordinary differential equations, in: *Proc. Int. Symp. on Symb. Algebr. Comput.*, ACM (Japan, 1990) 225–230.
[8] D. Grigoriev, Complexity of solving systems of linear equations over the rings of differential operators, in: *Proc. Int. Symp. Eff. Meth. in Algebraic Geometry* (Italy, 1990), Progress Mathematics, Vol. 94, (Birkhäuser, Boston, MA, 1991) 195–202.
[9] N. Jacobson, Pseudo-linear transformations, *Ann. Math.* **38**(2) (1937) 484–507.
[10] I. Kaplansky, *An Introduction to Differential Algebra* (Hermann, Paris, 1957).
[11] E. Kolchin, *Differential Algebra and Algebraic Groups* (Academic Press, New York, 1973).
[12] K. Mulmuley, A fast parallel algorithm to compute the rank of a matrix over an arbitrary field in: *Proc. 18 STOC ACM* (1986) 338–339.
[13] F. Ollivier, Standard Bases of Differential Ideals, in: Lecture Notes Computure Science, Vol. 508 (Springer, New York, 1991) 304–321.
[14] J.F. Ritt, *Differential Algebra*, in: Amer. Math. Soc. Colloq. Publ., Vol. 33 (American Mathematical Society, Providence, RI, 1950).